DISA
A Combat Support Agency

Mission Assurance FY12 Opportunities

DISA
A Combat Support Agency

DISA Strategy for Cyber Security

- **Evolved from:**
  - "Information Assurance" to "Mission Assurance"
  - Security focus to Operational focus -- recognizing that we operate in a Contested Battlespace
- **Evolving from:**
  - Compliance to Readiness
  - Manual to Machine-to-machine
- **Based on competitive acquisition of *enterprise-grade* commercial solutions integrated into the DoD architecture and reinforced by limited custom development**

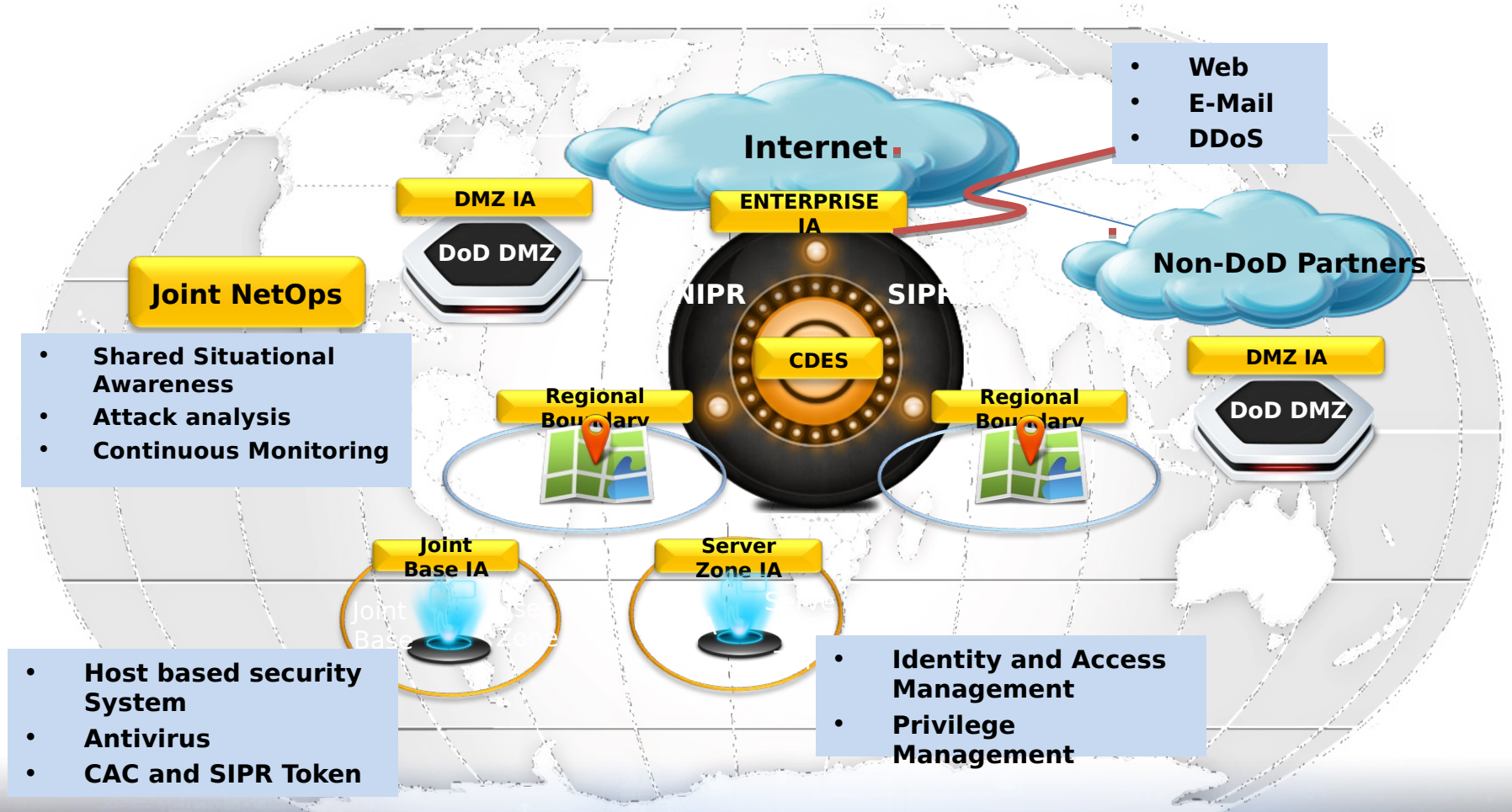
DISA
A Combat Support Agency

Mission Assurance Approach

- **Defensible Boundaries**
  - Enhance perimeter defenses
  - Cyber attack detection, diagnosis, reaction at network speed
- **Cyber COP**
  - "Blue Force"
    - Readiness status and Risk Scoring
  - "Red Forces"
    - Correlated attack detection integrated with intelligence picture
- **Safe Sharing (wikileaks mitigations)**
  - Insider Threat capability
  - Evolve directory, identity, and access control to

SecDef's "IT Efficiencies" provides an opportunity to save money and improve Cyber capabilities

Notional Security Architecture



SCM Development Support

- **Project** – Secure Configuration Management (SCM) Development Support
- **Anticipated Start Date** – 4th Quarter, FY12
- **Predecessor Contracts** – N/A
- **Anticipated Small Business Involvement** – TBD
- **Anticipated Contract Type** – CPFF

SCM program delivers enterprise capabilities to automate DoD Vulnerability and Secure Configuration Management Process, to include: host and network based scanning and discovery, continuous monitoring, automated security content (e.g., STIGs/IAVMs) management systems, continuous risk scoring using machine to machine reporting. These integrated and optimized enterprise IA applications and tools provide an automated process for risk management. This effort will provide development support for the integration of the SCM applications and databases into a single data warehouse.

DIBNET Development

Project – Defense Industrial Base Network (DIBNet) Development
Anticipated Start Date – 3rd Quarter, FY12
Predecessor Contracts – IATAC
Anticipated Small Business Involvement – TBD
Anticipated Contract Type – TBD
RFI to be released September 2011

The DIBNet is a development effort to increase capabilities to communicate both unclassified and classified information securely with DIB partners. Desire robust, user-friendly collaborative environment and threat information sharing capabilities.

NetOps Strategic Outreach Data Strategy

Project - NetOps Strategic Outreach Data Strategy
Anticipated Start Date - 2nd Quarter, FY12
Predecessor Contracts – none
Anticipated Small Business Involvement – TBD
Anticipated Contract Type – TBD
RFI to be released August 2011

Strategic Outreach provides the communications strategy to articulate DISA's NetOps mission, capabilities, and roadmap. Data Strategy engages with current and future NetOps projects to produce technology neutral NetOps data exchange standards.

IdAM Development & Sustainment Support

- **Project** – IdAM Development & Sustainment Support
- **Anticipated Start Date** – 1st Quarter, FY12
- **Predecessor Contracts** – Technica (contractor)
- **Anticipated Small Business Involvement** – Full and Open via GSA Alliant
- **Anticipated Contract Type** – FFP

This effort will increase the security posture of the DoD by providing a dynamic seamless security environment supporting Identity Management efforts. This effort includes development of reference implementations for access control decisioning and enforcement for the DoD using Attribute-Based Access Control (ABAC) concepts. DoD's net-centric information sharing environment, and evolution towards increased interoperability with other federal agencies and coalition partners, requires applications and systems to evolve their current authentication, authorization, and access

Privilege Management Solution

- **Project** – Privilege Management Solution
- **Anticipated Start Date** – 2nd Quarter, FY12
- **Predecessor Contracts** – N/A
- **Anticipated Small Business Involvement** – Full and Open via GSA eBuy
- **Anticipated Contract Type** – FFP

Identity Management capabilities, specifically Attribute Based Access Control. The primary area of focus is the procurement of one or more Commercial-Off-the-Shelf (COTS) solution(s) to provide access control capabilities and access to subject matter experts who will support development and provide ongoing support of the COTS solution(s). Solutions must use standards that work across DoD and are interoperable with the Global Information Grid (GIG) architecture. Acquisition of an Attribute-Based Access Control capability is the first step towards a future Policy Based Access Control (PBAC) capability.

Cross Domain Enterprise Services

Project – Cross Domain Enterprise Service (CDES)

- Enterprise Email
- File Transfer
- Chat

Anticipated Start Date – 3rd Quarter, FY12
Predecessor Contracts – none
Anticipated Small Business Involvement – TBD
Anticipated Contract Type – TBD
RFI to be released August 2011

CDES is seeking technologies that can serve the needs of the DoD enterprise for cross domain transfers, scale to support the DoD enterprise, operate within the enterprise environment, and realize cost efficiencies for the department.

DISA
A Combat Support Agency

Anti-Virus Recompete

- **Project** – Anti-Virus Recompete
- **Anticipated Start Date** – 1st Quarter, FY13
- **Predecessor Contracts** – En Pointe Gov, Inc. (McAfee reseller) and TVAR Solutions Inc. (Symantec reseller)
- **Anticipated Small Business Involvement** – Limited competition on the GSA FSS schedule (includes small businesses)
- **Anticipated Contract Type** – FFP

DISA maintains lifecycle support for DoD's enterprise anti-virus and anti-spyware products. The upcoming acquisition will provide maintenance of the existing anti-virus/anti-spyware licenses.

DISA
A Combat Support Agency

HBSS Follow-on Phase II

- **Project** – HBSS Follow-on Phase II
- **Anticipated Start Date** – 4th Quarter, FY13
- **Predecessor Contracts** – Current HBSS effort
- **Anticipated Small Business Involvement** – TBD
- **Anticipated Contract Type** – TBD

The HBSS solution suite is an enterprise-wide automated, standardized tool that provides host-based security, against both insider threats and external threats. DISA will pursue an open architecture to replace the current proprietary host based security solution. Solution must allow for integration of capabilities from other vendors and support the DoD enterprise.

DDoS Detect and React (DR)

Project – Distributed Denial of Service (DDoS) Detect and React (DR)
Anticipated Start Date – 4th Quarter, FY12
Predecessor Contracts – none
Anticipated Small Business Involvement – TBD
Anticipated Contract Type – TBD
Original RFI released 2009; **new RFI to be released** August 2011

DDOS Detect and React provides visibility into network behavior, alerts analysts to anomalous events and provides attack mitigation options.

DISA
A Combat Support Agency

On the Drawing Board

- Defense Enterprise Security Architecture
- Non-signature based attack detection
- Bootable media
- Mobile device security
- Advanced attack analysis
- Insider threat